PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-162680
(43)Date of publication of application : 06.06.2003

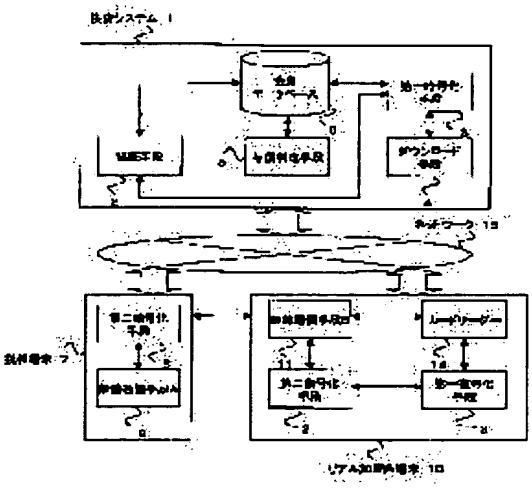
(51)Int.Cl. G06F 17/60
G09C 1/00

(21)Application number : 2001-362788
(22)Date of filing : 28.11.2001

(71)Applicant : JCB:KK
(72)Inventor : SHIMOKAWA TAKAHIRO

(54) SETTLEMENT SYSTEM AND METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a settlement system and a method for making settlement by a card using a portable terminal of portable telephone or the like.
SOLUTION: In the settlement system, data can be transmitted/received between the portable terminal and a real member store terminal through a network, and the system includes a member database, a first encryption means that encrypts card information using a predetermined first cipher key to create first encryption data, a download means that transmits software and the first encryption data for making settlement by a card to the portable terminal, and a credit decision means that receives, from the real member store, a telegraphic message edited from a plaintext that has been converted from the encrypted card information directly received from the portable terminal by decrypting the information using a first decoding key corresponding to the first cipher key, and, based on the received telegraphic message, makes a credit decision of whether or not making settlement by the card of a user is to be approved based on the member database.



LEGAL STATUS

[Date of request for examination] 22.10.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－162680
（P2003－162680A）
(43)公開日　平成15年6月6日(2003.6.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	４１４	Ｇ０６Ｆ　17/60	４１４	５Ｊ１０４
	２４２		２４２	
	５０６		５０６	
	５１２		５１２	
	ＺＥＣ		ＺＥＣ	

審査請求　未請求　請求項の数28　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願2001－362788(P2001－362788)

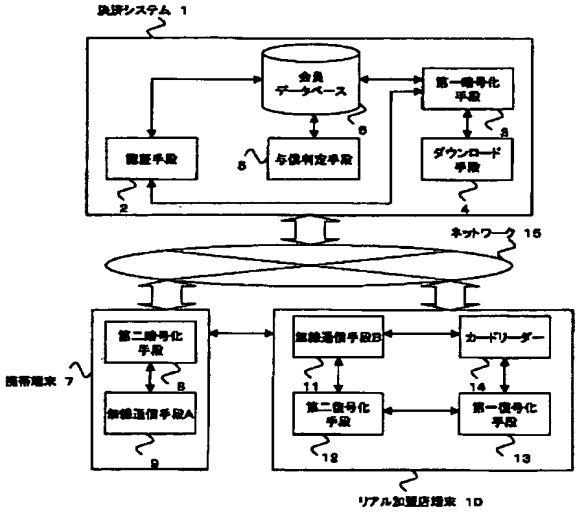
(22)出願日　平成13年11月28日(2001.11.28)

(71)出願人　593022629
株式会社ジェーシービー
東京都千代田区神田駿河台１丁目６番地
(72)発明者　下川　卓宏
東京都千代田区神田駿河台一丁目６番地
株式会社ジェーシービー情報ネットワーク部内
(74)代理人　100100402
弁理士　名越　秀夫　（外１名）

Ｆターム(参考)　5J104 NA02 NA35 PA07 PA10

(54)【発明の名称】　決済システム及び方法

(57)【要約】
【課題】携帯電話等の携帯端末を用いてカード決済を行う際の決済システム及び方法を提供することを目的とする。
【解決手段】決済システムに於いて、携帯端末とリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、会員データベースと、カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、カード決済を行わせる為のソフトウェア及び一次暗号化データを携帯端末に送信するダウンロード手段と、携帯端末から直接受信した暗号化されたカード情報を第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、平文から編集された電文をリアル加盟店端末から受信し、受信した電文に基づいてユーザのカード決済を承認するか否かの与信判定を、会員データベースに基づいて行う与信判定手段とを有する決済システムである。



1

【特許請求の範囲】

【請求項１】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信するダウンロード手段と、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有することを特徴とする決済システム。

【請求項２】前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信することを特徴とする請求項１に記載の決済システム。

【請求項３】前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項１又は請求項２に記載の決済システム。

【請求項４】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段と、前記二次暗号化データを前記リアル加盟店端末に直接送信する無線通信手段Ａとを有することを特徴とする携帯端末。

【請求項５】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Ｂと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカードリーダーとを有することを特徴とするリアル加盟店端末。

2

【請求項６】前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項５に記載のリアル加盟店端末。

【請求項７】前記リアル加盟店端末と前記携帯端末との間のデータの送受信は、ブルートゥース、赤外線通信のいずれかを含む無線通信を介して行うことを特徴とする請求項１から請求項６のいずれかに記載の決済システム。

【請求項８】ネットワークを介してカード決済を行う為の決済システムに於いて、前記カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信するダウンロード手段と、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有することを特徴とする決済システム。

【請求項９】前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗

号化データを前記ネットワークを介して送信することを特徴とする請求項８に記載の決済システム。

【請求項１０】前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項８又は請求項９に記載の決済システム。

【請求項１１】ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段を有することを特徴とするユーザ端末。

【請求項１２】ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカード情報処理手段とを有することを特徴とするバーチャル加盟店端末。

【請求項１３】前記ユーザ端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項１２に記載のバーチャル加盟店端末。

【請求項１４】前記第一復号キーは、予め前記決済システム及び／又は前記決済システムを有するカード会社から配布又は送信されていることを特徴とする請求項１から請求項１３のいずれかに記載の決済システム。

【請求項１５】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信し、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行うことを特徴とする決済方法。

【請求項１６】前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信することを特徴とする請求項１５に記載の決済方法。

【請求項１７】前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項１５又は請求項１６に記載の決済方法。

【請求項１８】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信することを特徴とする携帯端末。

【請求項１９】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済

システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Ｂと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記第一復号化手段に於いて変換した平文を電文に変換し送信することを特徴とするリアル加盟店端末。

【請求項２０】前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項１９に記載のリアル加盟店端末。

【請求項２１】前記リアル加盟店端末と前記携帯端末との間のデータの送受信は、ブルートゥース、赤外線通信のいずれかを含む無線通信を介して行うことを特徴とする請求項１５から請求項２０のいずれかに記載の決済方法。

【請求項２２】ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信し、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行うことを特徴とする決済方法。

【請求項２３】前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記ネットワークを介して送信することを特徴とする請求項２２に記載の決済方法。

【請求項２４】前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項２２又は請求項２３に記載の決済方法。

【請求項２５】ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成することを特徴とするユーザ端末。

【請求項２６】ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記変換した平文を電文に変換し送信することを特徴とするバーチャル加盟店端末。

【請求項２７】前記ユーザ端末が前記受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項２６に記載のバーチャル加盟店端末。

【請求項２８】前記第一復号キーは、予めカード会社から配布又は送信されていることを特徴とする請求項１５から請求項２７のいずれかに記載の決済方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯電話、ＰＨＳ等の携帯端末又はネットワークを介してカード決済を行う際の決済システム及び方法に関する。

【０００２】

【従来の技術】従来、商品等の購入を行う際にはその決済手段として現金決済の他に、クレジットカード、デビットカード等（以下、カード等）を用いて決済を行う方法（以下、カード決済）が存在している。これは商品等の購入を行う際に、カード等を提示し署名、暗証番号等によって正当なるカード等の所有者であるかの判別後、決済を行う方法である。

【０００３】更に近年の通信技術等の技術発達に伴い、自動販売機等の従来ではカード等による決済が行えなかった機器に於いても、携帯端末を用いることによってカード等による決済を行う方法が提案されている。

【０００４】上記の方法の一例が特開２００１－１３４６８４号に開示されている。この公開公報に開示されている発明は、自動販売機等の機器にカード決済を行う装置を取り付け、前記装置と携帯電話との間で無線通信を介してデータの送受信を行い、カード等による決済を実現するものである。

【０００５】

【発明が解決しようとする課題】特開２００１－１３４６８４号公開公報に開示されている発明を用いた場合では、携帯電話とカード決済を行う装置との間での無線通信のセキュリティ面に問題点が存在している。即ち、例えば公知の無線通信技術であるブルートゥース、無線ＬＡＮ等の電波を用いた場合では、携帯電話から全周囲に（携帯電話を中心として同心円上に）情報が発信されるので、不必要な方向に対しても情報が発信されてしまうこととなる。従って、悪意を有する者がこの情報を傍受して悪用することも可能である。

【０００６】更に電波以外の、例えば指向性がある赤外線通信（ＩｒＤＡ）等を用いた方法もあるが、この場合には不必要な方向に対して情報が発信される問題は解決できるが、同方向の延長線上に悪意を有する者が存在した場合には、同様にこの情報を傍受して悪用することも可能である。

【０００７】更に携帯電話を忘れる、落とす等は日常生活に於いて起こりえることであるが、上記公開公報に開示されている発明を単に用いた場合では、携帯電話を取得した第三者がそれを悪用して決済を行うことも可能である。

【０００８】

【課題を解決するための手段】カード決済に於いて重要なことはセキュリティ面にある。つまり携帯端末からカード決済を行う装置に対して情報を送信した場合に、その情報が第三者によって傍受され悪用される可能性、落とした携帯電話等でそれを用いて第三者に悪用される可能性等である。

【０００９】本発明者は上記問題点に鑑み、このセキュリティ面を重視することによる、より有効性のあるカード決済を行う決済システム及び方法を発明した。

【００１０】更に携帯端末／ユーザ端末を用いた場合、従来はカード決済を行う装置（以下、カードリーダー）とカード会社とのカード決済用の情報処理システムを変更する必要があったが、本発明を用いることによって、従来のカードリーダーに無線通信とデータ復号化のユニットを単に接続するのみで、カードリーダーとカード会社とのカード決済用の情報処理システムについては何らの変更を加える必要性がない。従って、カード決済用の情報処理システムの変更の手間負担、コスト負担を回避することが可能となる。

【００１１】請求項１の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信するダウンロード手段と、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有する決済システムである。

【００１２】請求項１５の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信し、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う決済方法である。

【００１３】請求項２の発明は、前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する決済システムである。

【００１４】請求項１６の発明は、前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを

作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する決済方法である。

【００１５】請求項３の発明は、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済システムである。

【００１６】請求項１７の発明は、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済方法である。

【００１７】請求項１から請求項３及び請求項１５から請求項１７の発明によって、セキュリティ面が向上した携帯端末を用いたカード決済の決済システムが可能となる。又従来のカード決済システムをそのまま用いることが可能となるので、システム導入の際に発生するコストを安価に抑えることが可能となる。尚、本明細書に於いて編集とは、平文を単にそのまま電文にする、平文に所定の事項を追加して電文にする、平文を加工して同内容の電文にする、又前記同内容の電文に所定の事項を更に追加する等を意味している。

【００１８】請求項４の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段と、前記二次暗号化データを前記リアル加盟店端末に直接送信する無線通信手段Ａとを有する携帯端末である。

【００１９】請求項１８の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する携帯端末である。

【００２０】請求項４及び請求項１８の発明によって、決済システムから送信された一次暗号化データを更に暗号化してリアル加盟店端末に送信することが可能となり、これによって、無線通信が傍受されても２重の暗号化が施されている為、解読が困難となり、セキュリティ面の向上に繋がる。

【００２１】請求項５の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Ｂと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカードリーダーとを有するリアル加盟店端末である。

【００２２】請求項６の発明は、前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するリアル加盟店端末である。

【００２３】請求項１９の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Ｂと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記第一復号化手段に於いて変換した平文を電文に変換し送信するリアル加盟店端末である。

【００２４】請求項２０の発明は、前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作

成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するリアル加盟店端末である。

【００２５】請求項５と請求項６及び請求項１９と請求項２０の発明によって、携帯端末から受信した暗号化されたカード情報を復号化し、それを従来通りのカードリーダーで決済システムに送信する為、カード決済に大幅な変更を加える必要性がなく、本発明の決済システムを安価に導入することが可能となる。

【００２６】請求項８の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、前記カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信するダウンロード手段と、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有する決済システムである。

【００２７】請求項９の発明は、前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記ネットワークを介して送信する決済システムである。

【００２８】請求項１０の発明は、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済システムである。

【００２９】請求項２２の発明は、ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信し、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う決済方法である。

【００３０】請求項２３の発明は、前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記ネットワークを介して送信する決済方法である。

【００３１】請求項２４の発明は、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済方法である。

【００３２】請求項８から請求項１０及び請求項２２から請求項２４の発明によって、セキュリティ面が向上したネットワークを介したカード決済の決済システムが可能となる。又従来のカード決済システムをそのまま用いることが可能となるので、システム導入の際に発生するコストを安価に抑えることが可能となる。

【００３３】請求項１１の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段を有するユーザ端末である。

【００３４】請求項２５の発明は、ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次

暗号化データを作成するユーザ端末である。

【００３５】請求項１１及び請求項２５の発明によって、決済システムから送信された一次暗号化データを更に暗号化してバーチャル加盟店端末に送信することが可能となり、これによって、ネットワーク上に於いてユーザ端末とバーチャル加盟店端末との通信が傍受されても２重の暗号化が施されている為、解読が困難となり、セキュリティ面の向上に繋がる。

【００３６】請求項１２の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカード情報処理手段とを有するバーチャル加盟店端末である。

【００３７】請求項１３の発明は、前記ユーザ端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するバーチャル加盟店端末である。

【００３８】請求項２６の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記変換した平文を電文に変換し送信するバーチャル加盟店端末である。

【００３９】請求項２７の発明は、前記ユーザ端末が前記受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するバーチャル加盟店端末である。

【００４０】請求項１２と請求項１３及び請求項２６と請求項２７の発明によって、ユーザ端末から受信した暗号化されたカード情報を復号化し、それを従来通りのカード情報処理手段で決済システムに送信する為、カード決済に大幅な変更を加える必要性がなく、本発明の決済システムを安価に導入することが可能となる。

【００４１】請求項１４の発明は、前記第一復号キーは、予め前記決済システム及び／又は前記決済システムを有するカード会社から配布又は送信されている決済システムである。

【００４２】請求項２８の発明は、前記第一復号キーは、予めカード会社から配布又は送信されている決済方法である。

【００４３】

【発明の実施の形態】本発明の実施態様の一例を図を用いて詳細に説明する。図１及び図２は本発明の決済システム１のシステム構成の一例である。図１は、実在する店舗（以下、リアル加盟店とする）に於いてユーザ（カード等を用いた決済を行う者）が当該店舗に赴きカード決済を行う場合を示し、図２は、オンラインショッピング等のネットワーク１５上に存在する店舗（以下、バーチャル加盟店とする）に於いてユーザがネットワーク１５を介してカード決済を行う場合のシステム構成を示した図である。

【００４４】まず図１に於けるユーザがリアル加盟店で決済システム１を用いる場合を説明する。決済システム１は、ユーザが有する携帯端末７とリアル加盟店が有するリアル加盟店端末１０と決済システム１とがネットワーク１５を介してデータの送受信が可能である。又携帯端末７の無線通信手段Ａ９とリアル加盟店端末１０の無線通信手段Ｂ１１とは、ブルートゥース、ＩｒＤＡ等の無線通信を行う手段であって、直接データの送受信が可能である。

【００４５】決済システム１は、カード決済を行うカード会社等が有するシステムであって、認証手段２と第一暗号化手段３とダウンロード手段４と与信判定手段５と会員データベース６とを有している。

【００４６】認証手段２は、携帯端末７からアクセス要求を受信した際に正当なるユーザであるか否かの認証を行う手段である。この認証の際には、ユーザ本人を認証する為の認証情報（ＩＤやパスワード等）、電話番号、住所等を用いて行う。

【００４７】第一暗号化手段３は、ユーザが有する携帯端末７に対してカード情報（ユーザのカード番号とカー

ド有効期限）を予め定められた暗号化方法によって、第一暗号キーで暗号化する手段である。この暗号化方法には公知のＤＥＳ等を用いた共通鍵暗号方式、ＲＳＡ等を用いた公開鍵暗号方式が該当する。即ちユーザがカード決済に用いるカード情報（例えば、「３５４０１２３４５６７８９」「０１／０５」最初の括弧がカード番号、最後の括弧が有効期限を示している）を予め定められた第一暗号キーで暗号化し、一次暗号化データ（例えば、「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／○×」）を作成する。

【００４８】ダウンロード手段４は、携帯端末７とリアル加盟店端末１０との間で直接データの送受信を行いカード決済を行わせる為のソフトウェアを、携帯端末７に送信する手段である。尚、セキュリティ性を向上させる為に、第一暗号化手段３で暗号化された一次暗号化データを更にワンタイムパスワード等を用いることによって携帯端末７で暗号化させる為のプログラム（第二暗号化手段８）を、当該ソフトウェアに組み込んでも良い。

【００４９】与信判定手段５は、リアル加盟店端末１０からネットワーク１５を介して送信されたカード情報を受信し、当該カード決済の対象となるユーザの限度額等を会員データベース６を参照し、ユーザのカード決済を承認するか否かの与信判定を行う手段である。つまり従来のカード決済に於ける与信判定と同等の処理を行う手段である。

【００５０】会員データベース６は、決済システム１を利用するユーザの情報を格納しているデータベースである。ユーザの情報の一例としては、本人を認証する情報（ＩＤやパスワード）、ユーザに関する情報（氏名、住所、電話番号等）、カード情報（カード番号、カード有効期限）等を格納しているデータベースである。

【００５１】携帯端末７は、ネットワーク１５機能を有する携帯電話、ＰＨＳ、ＰＤＡ、ノート型パソコン等であるがこれに限定されず、通常のパーソナルコンピュータであっても良い。

【００５２】携帯端末７は、第二暗号化手段８と無線通信手段Ａ９とを有する。

【００５３】第二暗号化手段８は、決済システム１のダウンロード手段４から受信したソフトウェアに組み込まれている、第一暗号化手段３で暗号化された一次暗号化データを更にワンタイムパスワード等の第二暗号キーを用いることによって更に暗号化し、二次暗号化データを作成する為のプログラムである。ここでワンタイムパスワードとして、一次暗号化データを、第二暗号化手段８に於いて暗号化する時刻等を第二暗号キーとして用いることによって暗号化する方法をその一例とするが、それ以外であっても良い。

【００５４】例えば、一次暗号化データを暗号化する時刻を第二暗号キーとしており、その時刻が１４時３３分であった場合には、第二暗号キーが「１４３３」とな

り、一次暗号化データが「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／◎×」であった場合、これを第二暗号化手段８に於いて「ｘｙｚｙ＄”０ｑ１！＃＠＊＜Ｎ？＆＃！ｐ」と二次暗号化データを作成する。

【００５５】無線通信手段Ａ９は、リアル加盟店端末１０が有する無線通信手段Ｂ１１と直接データの送受信が可能なデータ送受信手段であって、ブルートゥース、ＩｒＤＡ等の公知の無線通信手段を示す。上記例の場合では、二次暗号化データ「ｘｙｚｙ＄”０ｑ１！＃＠＊＜Ｎ？＆＃！ｐ」を送信する。

【００５６】リアル加盟店端末１０は、リアル店舗が有しているカード決済をカード会社との間でデータ処理する為のシステムであって、無線通信手段Ｂ１１と第二復号化手段１２と第一復号化手段１３とカードリーダー１４とを有している。

【００５７】無線通信手段Ｂ１１は、携帯端末７が有する無線通信手段Ａ９と直接データの送受信が可能なデータ送受信手段であって、ブルートゥース、ＩｒＤＡ等の公知の無線通信手段を示す。上記例の場合では、二次暗号化データ「ｘｙｚｙ＄”０ｑ１！＃＠＊＜Ｎ？＆＃！ｐ」を受信する。

【００５８】第二復号化手段１２は、携帯端末７の第二暗号化手段８に於いて暗号化され、無線通信手段Ｂ１１が携帯端末７から受信した二次暗号化データを、第二復号キーを用いて復号化する為の手段である。第二復号キーは、第二暗号キーを復号する為の復号キーを意味し、例えば第二暗号キーが時刻の場合には、第二復号キーも時刻となる。第二暗号化手段８に於いて暗号化する時刻が第二暗号キーの場合には、当該時刻が第二復号キーとなる。つまり、第二暗号化手段８に於いて一次暗号データを暗号化し、二次暗号化データを作成する時刻と、無線通信手段Ａ９及び無線通信手段Ｂ１１を介してリアル加盟店端末１０に於いて二次暗号化データを携帯端末７から受信し、第二復号化手段１２に於いて復号する際の時刻とは、ほぼ同一であるので当該時刻を用いても正常に暗号化／復号化が可能となる。

【００５９】例えば上記例の場合では、無線通信手段Ｂ１１が受信した二次暗号化データ「ｘｙｚｙ＄”０ｑ１！＃＠＊＜Ｎ？＆＃！ｐ」を第二復号キー「１４３３」で一次暗号化データ「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／○×」に復号化する。

【００６０】第一復号化手段１３は、第二復号化手段１２に於いて二次暗号化データが復号され、一次暗号データとなったデータを、更に第一復号キーを用いて復号化する為の手段である。第一復号キーは、第一暗号キーを復号する為の復号キーを意味し、決済システム１の第一暗号化手段３で暗号化された一次暗号データを復号化するものである。つまり、一次暗号データを復号化することによって、ユーザのカード決済に用いるカード情報を平文化することが可能となる。又第一暗号キーは、予め

決済システム１（又はカード会社）からＣＤ－ＲＯＭ等の電子記録媒体を用いて配布又はデータとして送信されており、場合によっては予めチップ等に書き込まれていても良い。

【００６１】上記例の場合では、第二復号化手段１２に於いて復号化した一次暗号化データ「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／○×」を、予め定められている第一復号キーで復号化することによって、カード情報を「３５４０１２３４５６７８９」に平文化することなる。

【００６２】カードリーダー１４は、従来のカード決済を行う際の磁気式クレジットカード等を読み取る為のカードリーダー１４と同等の機能を有する処理システムであり、ネットワーク１５を介してカード会社が有する決済システム１との間で第一復号化手段１３によって平文化されたカード情報の送受信を行い、カード決済を行う手段である。

【００６３】次に図２に於けるユーザがバーチャル加盟店で決済システム１を用いる場合を説明する。尚図１のシステム構成と同一部分については簡略化の為、説明を省略する。決済システム１は、ユーザが有するユーザ端末１８とバーチャル加盟店が有するバーチャル加盟店端末１７と決済システム１とがネットワーク１５を介してデータの送受信が可能である。

【００６４】決済システム１の認証手段２は、ユーザ端末１８からアクセス要求を受信した際に正当なるユーザであるか否かの認証を行う手段である。

【００６５】第一暗号化手段３は、ユーザが有するユーザ端末１８に対してカード情報（ユーザのカード番号とカード有効期限）を予め定められた暗号化方法によって、第一暗号キーで暗号化する手段である。暗号化する方法等は、図１と同様である。

【００６６】ダウンロード手段４は、ユーザ端末１８とバーチャル加盟店端末１７との間で直接データの送受信を行いカード決済を行わせる為のソフトウェアを、ユーザ端末１８に送信する手段である。

【００６７】与信判定手段５は、バーチャル加盟店端末１７からネットワーク１５を介して送信されたカード情報を受信し、当該カード決済の対象となるユーザの限度額等を会員データベース６を参照し、ユーザのカード決済を承認するか否かの与信判定を行う手段である。

【００６８】会員データベース６は、決済システム１を利用するユーザの情報を格納しているデータベースである。

【００６９】ユーザ端末１８は、ネットワーク１５機能を有する携帯電話、ＰＨＳ、ＰＤＡ、パーソナルコンピュータを示す。

【００７０】ユーザ端末１８は、第二暗号化手段８を有する。

【００７１】第二暗号化手段８は、決済システム１のダウンロード手段４から受信したソフトウェアに組み込まれている、第一暗号化手段３で暗号化された一次暗号化データを更にワンタイムパスワード、ＳＳＬで用いる暗号キー等の第二暗号キーを用いることによって更に暗号化し、二次暗号化データを作成する為のプログラムである。第二暗号キー等は図１と同様である。

【００７２】バーチャル加盟店端末１７は、バーチャル店舗に於けるカード決済をカード会社との間でデータ処理する為のシステムであって、第二復号化手段１２と第一復号化手段１３とカード情報処理手段１６とを有している。バーチャル加盟店端末１７は、バーチャル店舗が有していても良いし、それ以外の他の者が有していても良い。

【００７３】第二復号化手段１２は、ユーザ端末１８の第二暗号化手段８に於いて暗号化され、ネットワーク１５を介してユーザ端末１８から受信した二次暗号化データを、第二復号キーを用いて復号化する為の手段である。第二復号キー等は、図１と同様である。

【００７４】第一復号化手段１３は、第二復号化手段１２に於いて二次暗号化データが復号され、一次暗号データとなったデータを、更に第一復号キーを用いて復号化する為の手段である。第一復号キー等は、図１と同様である。

【００７５】カード情報処理手段１６は、従来のカード決済を行う際と同等の機能を有する処理システムであり、ネットワーク１５を介してカード会社が有する決済システム１との間で第一復号化手段１３によって平文化されたカード情報の送受信を行い、カード決済を行う手段である。

【００７６】

【実施例】次に本発明のプロセスの流れの一例を図３及び図４のフローチャート図と図１及び図２のシステム構成図とを用いて詳細に説明する。図３及び図４は、携帯端末７又はユーザ端末１８と、リアル加盟店端末１０又はバーチャル加盟店端末１７との間で直接データの送受信を行いカード決済を行わせる（第二暗号化手段８を含む）為のソフトウェアを、携帯端末７又はユーザ端末１８に送信する（ダウンロードさせる）場合のフローチャート図である。

【００７７】まず図３に示した、ソフトウェアを携帯端末７又はユーザ端末１８に送信する際のプロセスの流れの一例を示す。本プロセスは、予めユーザのカード情報を第一暗号化手段３に於いて一次暗号化データとし、当該一次暗号化データをインプリメントしたソフトウェアを携帯端末７又はユーザ端末１８に送信する場合である。

【００７８】ユーザは自らが有する携帯端末７又はユーザ端末１８からネットワーク１５を介して決済システム１にアクセスする（Ｓ１００）。Ｓ１００に於いて携帯端末７又はユーザ端末１８と決済システム１との間で接

続が確立後、ユーザは携帯端末７又はユーザ端末１８から決済システム１の認証手段２に対してＩＤ、パスワード等の認証情報を送信する（Ｓ１１０）。

【００７９】Ｓ１１０に於いて送信された認証情報を受信した認証手段２は、前記認証情報を、会員データベース６に格納している認証情報に基づいて認証を行い、正規のユーザであるか否かの認証を行う（Ｓ１２０）。

【００８０】Ｓ１２０の認証の結果、認証が出来なかった場合には認証手段２は携帯端末７又はユーザ端末１８に対してエラーメッセージを送信する（Ｓ１３０）。Ｓ１２０に於いて認証が行えた場合には、第一暗号化手段３が、当該認証を行ったユーザの会員データベース６に格納しているカード情報を予め定められている第一暗号キーで暗号化し、一次暗号化データを作成する（Ｓ１４０）。

【００８１】例えばカード情報が「３５４０１２３４５６７８９」「０１／０５」であった場合、予め定められた第一暗号キーで暗号化し、一次暗号化データ（例えば、「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／○×」）を作成する。

【００８２】Ｓ１４０に於いて作成した一次暗号化データを、前記ソフトウェアにインプリメントしてダウンロード手段４が、当該ソフトウェアを携帯端末７又はユーザ端末１８に送信し、ダウンロードさせる（Ｓ１５０）。

【００８３】Ｓ１５０に於いてネットワーク１５を介して携帯端末７又はユーザ端末１８に送信したソフトウェアを携帯端末７又はユーザ端末１８が格納することによって、図３のプロセスを終了する。

【００８４】次に図４に示した、ソフトウェアを携帯端末７又はユーザ端末１８に送信する際のプロセスの流れの一例を示す。本プロセスは、ユーザのカード情報を除いた部分（携帯端末７又はユーザ端末１８とリアル加盟店端末１０又はバーチャル加盟店端末１７との間で直接データの送受信を行いカード決済を行わせる（第二暗号化手段８を含む）部分）のみのソフトウェアをまず送信し、その後ユーザからの要求に伴って、ユーザのカード情報を第一暗号化手段３に於いて暗号化することにより一次暗号化データを作成し、当該一次暗号化データをダウンロードが別途携帯端末７又はユーザ端末１８に送信し、携帯端末７又はユーザ端末１８に於いて当該ソフトウェアに一次暗号化データを組み込む方法である。従ってソフトウェアと一次暗号化データのダウンロードは同時には行わなくても良い。

【００８５】ユーザは自らが有する携帯端末７又はユーザ端末１８からネットワーク１５を介して決済システム１にアクセスする（Ｓ２００）。Ｓ２００に於いて携帯端末７又はユーザ端末１８と決済システム１との接続が確立後、ユーザは携帯端末７又はユーザ端末１８からダウンロード手段４に対して、ユーザのカード情報を除いた部分（携帯端末７又はユーザ端末１８とリアル加盟店端末１０又はバーチャル加盟店端末１７との間で直接データの送受信を行いカード決済を行わせる（第二暗号化手段８を含む）部分）のみのソフトウェアのダウンロードの要求を送信する（Ｓ２１０）。

【００８６】Ｓ２１０に於けるダウンロードの要求を受信後、ダウンロード手段４は、ユーザのカード情報を除いた部分のみのソフトウェアを携帯端末７又はユーザ端末１８に送信し、ダウンロードを行わせる（Ｓ２２０）。

【００８７】Ｓ２２０に於いて送信されたカード情報を除いた部分のみのソフトウェアを携帯端末７又はユーザ端末１８に於いて受信、格納し、その後（同時でなくとも後であっても良い）携帯端末７又はユーザ端末１８を用いたカード決済を行う前までに携帯端末７又はユーザ端末１８から決済システム１に再度アクセスし、携帯端末７又はユーザ端末１８から認証手段２に認証情報を送信し（Ｓ２３０）、正規のユーザであるか否かの認証を認証手段２に行わせる。認証の方法は図３の場合と同様で良い。

【００８８】Ｓ２３０に於いて送信された認証情報を受信した認証手段２は、認証を行い正規のユーザであるか否かの認証を行う（Ｓ２４０）。

【００８９】Ｓ２４０の認証の結果、認証できなかった場合には、認証手段２は携帯端末７又はユーザ端末１８に対してエラーメッセージを送信する（Ｓ２５０）。Ｓ２４０に於いて認証できた場合には第一暗号化手段３が、当該認証を行ったユーザのカード情報を予め定められている第一暗号キーを用いて暗号化し一次暗号化データを作成する（Ｓ２６０）。

【００９０】一次暗号化データを作成後、ダウンロード手段４がネットワーク１５を介して一次暗号化データを携帯端末７又はユーザ端末１８に送信する（Ｓ２７０）。Ｓ２７０に於いてネットワーク１５を介して送信された一次暗号化データを携帯端末７又はユーザ端末１８に於いて受信後、携帯端末７又はユーザ端末１８が受信した一次暗号化データを、Ｓ２２０に於いて格納したソフトウェアに組み込み、携帯端末７又はユーザ端末１８に於いて格納することによって図４のプロセスを終了する。

【００９１】次に、図３又は図４のプロセスを経てソフトウェアをダウンロード後、当該ソフトウェアを用いてカード決済を行う際のプロセスの流れの一例を示す。まず図５及び図６に於いて、リアル加盟店に於ける場合を説明する。

【００９２】リアル加盟店に於けるリアル加盟店端末１０には、予め決済システム１又はカード会社からリアル加盟店端末１０の第一復号化手段１３に於ける第一復号キーが配布され組み込まれている。ここで第一復号キーとは、決済システム１の第一暗号化手段３に於いてカー

ド情報を一次暗号化データに暗号化する第一暗号キーに対応し、一次暗号化データを平文のカード情報に復号化する復号キーを示す。又第一復号キーのリアル加盟店端末１０に対する配布は、リアル加盟店端末１０のチップに予め記憶させておく、ネットワーク１５を介して決済システム１からリアル加盟店端末１０の第一区豪華手段に送信する、ＣＤ－ＲＯＭ等の記録媒体による配布等がある。

【００９３】ユーザがリアル加盟店端末１０に於いて決済を行う場合には、当該ソフトウェアを格納した携帯端末７のソフトウェアの一覧から、当該カード決済用のソフトウェア（図３又は図４でダウンロードしたソフトウェア）を起動する（Ｓ３００）。

【００９４】ソフトウェア起動後、当該ソフトウェアを正当に使用できるユーザか否かの判定を行う為、パスワード等の認証情報を入力させる（Ｓ３１０）。認証を行う為の認証画面の一例を図９に示す。この際に、複数のカード会社のカード決済が行えるように、その種類の選択（カード会社の選択）を行わせても良い。

【００９５】Ｓ３１０に於いて入力した認証情報が正当であるか否かの判定を行い（Ｓ３２０）、不当な入力であれば再度入力を促す。又正当なる入力であれば、カードの正当なる使用者であると見なして、購入意思確認画面を起動する。図１０に購入意思確認画面の一例を示す。

【００９６】ユーザの購入意思を確認後（購入意思確認画面の「送信」ボタンを押す等）、Ｓ１５０に於いてダウンロードしたソフトウェアに組み込まれた一次暗号化データ又はＳ２７０に於いて決済システム１から送信され携帯端末７に於いて受信した一次暗号化データを、携帯端末７の第二暗号化手段８に於いて第二暗号キーを用いて更に暗号化し二次暗号化データを作成する（Ｓ３３０）。

【００９７】例えば一次暗号化データが「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／◎×」であって、その一次暗号化データを第二暗号化手段８に於いて暗号化する時刻が１４時３３分であった場合（ワンタイムパスワード（第二暗号キー）として暗号化する時刻を用いている場合）には第二暗号キーが「１４３３」となり、その結果第二暗号化手段８に於いて一次暗号化データが更に「ｘｙｚｙ＄”０ｑｌ！＃＠＊＜Ｎ？＆＃！ｐ」と暗号化されることとなる。

【００９８】Ｓ３３０に於いて二次暗号化データを作成後、携帯端末７の無線通信手段Ａ９を介して二次暗号化データをリアル加盟店端末１０に対して直接送信する（Ｓ３４０）。

【００９９】Ｓ３４０に於いて無線通信手段Ａ９から送信された二次暗号化データを、リアル加盟店端末１０の無線通信手段Ｂ１１に於いて受信後、第二復号化手段１２が二次暗号化データを第二復号キーを用いて復号化する（Ｓ３５０）。

【０１００】上記例の場合、無線通信手段Ｂ１１に於いて受信した二次暗号化データが「ｘｙｚｙ＄”０ｑｌ！＃＠＊＜Ｎ？＆＃！ｐ」であって、その二次暗号化データを第二復号化手段１２に於いて復号化する時刻が１４時３３分であるので、第二復号キーが「１４３３」となり、その結果第二復号化手段１２に於いて二次暗号化データが「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／◎×」と一次暗号化データに復号される。

【０１０１】第二復号化手段１２に於いて一次暗号化データに復号後、第一復号化手段１３に於いて、一次暗号化データを第一復号キーを用いて平文に復号化する（Ｓ３６０）。

【０１０２】上記例の場合、一次暗号化データが「＊％＄＃＝＆％＄＆＃＠＋｝｛－＋－／◎×」であるので、予め決済システム１又はカード会社から配布された第一復号キーを用いて復号化し、「３５４０１２３４５６７８９」「０１／０５」とカード情報を平文化することとなる。

【０１０３】第一復号化手段１３に於いて復号後、平文化したカード情報をリアル加盟店端末１０のカードリーダー１４が、正規のカードデータとして復号されているか否かの精査を行い（Ｓ３７０）、精査の結果何らかの異常が発生している場合には、エラーメッセージを無線通信手段Ｂ１１を介して携帯端末７に送信する（Ｓ３８０）。携帯端末７の無線通信手段Ａ９は、無線通信手段Ｂ１１から受信したエラーメッセージを表示し通知する。

【０１０４】Ｓ３７０の精査の結果異常がなければ、カードリーダー１４が平文化されたカードデータに基づいて電文を編集して、決済システム１に電文を送信する（Ｓ３９０）。ここで電文とは従来の磁気式クレジットカードを用いたカード決済と同様に、カード情報を予め定められた形式に変換し、購入商品等のカード決済に対する付随情報と共にカード会社に於いて決済する際の公知のフォーマットに対応したデータをいい、従来のカード決済の際のカードリーダー１４からカード会社に対して送信しているデータと同様のデータを示す。

【０１０５】リアル加盟店端末１０からネットワーク１５を介して送信された電文を受信した決済システム１の与信判定手段５は、会員データベース６を参照して当該ユーザに対してカード決済を行っても良いか否かの与信判定を会員データベース６に格納している限度額等の情報に基づいて行い（Ｓ４００）、限度額超過等の理由から決済を認めない場合には、与信拒否報告を与信判定手段５がリアル加盟店端末１０のカードリーダー１４に送信する。

【０１０６】与信拒否報告を受信したカードリーダー１４は、無線通信手段Ｂ１１を介して携帯端末７に与信拒否報告を送信する（Ｓ４１０）。Ｓ４１０に於いて送信

された与信拒否報告を携帯端末７の無線通信手段Ａ９で受信すると、携帯端末７上に於いて当該ソフトウェアが与信が拒否された旨の与信拒否画面を表示する（Ｓ４２０）。与信拒否画面の一例を図１１に示す。

【０１０７】Ｓ４００の判定の結果、当該ユーザに対して決済を認める場合には、与信許可報告を与信判定手段５がリアル加盟店端末１０のカードリーダー１４に送信する。与信許可報告を受信したカードリーダー１４は、無線通信手段Ｂ１１を介して携帯端末７に与信許可報告を送信する（Ｓ４３０）。Ｓ４３０に於いて送信された与信許可報告を携帯端末７の無線通信手段Ａ９で受信すると、携帯端末７上に於いて当該ソフトウェアが与信が許可され、決済が終了した旨の完了画面を表示する（Ｓ４４０）。図１２に完了画面の一例を示す。

【０１０８】このように、Ｓ３００からＳ４４０の一連のプロセスを実行することによって、又リアル加盟店端末１０では従来のカードリーダー１４に加えて、単に無線通信手段Ｂ１１と第一復号化手段１３、第二復号化手段１２を併設するのみで、従来よりもセキュリティ性が向上し、且つカードリーダー１４からカード会社に於けるカード決済の仕組みには何らの変化も加えずにその処理が可能となる。

【０１０９】次に図７及び図８に於けるネットワーク１５上のバーチャル店舗に於いて決済を行う場合のプロセスの流れの一例を図２のシステム構成図を用いて詳細に説明する。

【０１１０】バーチャル加盟店端末１７には、予め決済システム１又はカード会社からバーチャル加盟店端末１７の第一復号化手段１３に於ける第一復号キーが配布され組み込まれている。ここで第一復号キーとは、決済システム１の第一暗号化手段３に於いてカード情報を一次暗号化データに暗号化する第一暗号キーに対応し、一次暗号化データを平文のカード情報に復号化する復号キーを示す。又第一復号キーのバーチャル加盟店端末１７に対する配布は、バーチャル加盟店端末１７のチップに予め記憶させておく、ネットワーク１５を介して決済システム１からバーチャル加盟店端末１７の第一区豪華手段に送信する、ＣＤ－ＲＯＭ等の記録媒体による配布等がある。

【０１１１】ユーザがバーチャル加盟店端末１７に於いて決済を行う場合には、当該ソフトウェアを格納したユーザ端末１８のソフトウェアの一覧から、当該カード決済用のソフトウェア（図３又は図４でダウンロードしたソフトウェア）を起動する（Ｓ５００）。

【０１１２】ソフトウェア起動後、当該ソフトウェアを正当に使用できるユーザか否かの判定を行う為、パスワード等の認証情報を入力させる（Ｓ５１０）。この際に、複数のカード会社のカード決済が行えるように、その種類の選択（カード会社の選択）を行わせても良い。

【０１１３】Ｓ５１０に於いて入力した認証情報が正当であるか否かの判定を行い（Ｓ５２０）、不当な入力であれば再度入力を促す。又正当なる入力であれば、カードの正当なる使用者であると見なして、購入意思確認画面を起動する。

【０１１４】ユーザの購入意思を確認後（購入意思確認画面の「送信」ボタンを押す等）、Ｓ１５０に於いてダウンロードしたソフトウェアに組み込まれた一次暗号化データ又はＳ２７０に於いて決済システム１から送信されユーザ端末１８に於いて受信した一次暗号化データを、ユーザ端末１８の第二暗号化手段８に於いて第二暗号キーを用いて更に暗号化し二次暗号化データを作成する（Ｓ５３０）。

【０１１５】例えば一次暗号化データが「＊％＄＃＝＆％＄＆＃@＋｝｛－＋－／◎×」であって、その一次暗号化データを第二暗号化手段８に於いて暗号化する時刻が１４時３３分であった場合（ワンタイムパスワード（第二暗号キー）として暗号化する時刻を用いている場合）には第二暗号キーが「１４３３」となり、その結果第二暗号化手段８に於いて一次暗号化データが更に「ｘｙｚｙ＄”０ｑｌ！＃@＊＜Ｎ？＆＃！ｐ」と暗号化されることとなる。

【０１１６】Ｓ５３０に於いて二次暗号化データを作成後、二次暗号化データをネットワーク１５を介してバーチャル加盟店端末１７に対して送信する（Ｓ５４０）。

【０１１７】Ｓ５４０に於いて送信された二次暗号化データを、バーチャル加盟店端末１７に於いて受信後、第二復号化手段１２が二次暗号化データを第二復号キーを用いて復号化する（Ｓ５５０）。

【０１１８】上記例の場合、受信した二次暗号化データが「ｘｙｚｙ＄”０ｑｌ！＃@＊＜Ｎ？＆＃！ｐ」であって、その二次暗号化データを第二復号化手段１２に於いて復号化する時刻が１４時３３分であるので、第二復号キーが「１４３３」となり、その結果第二復号化手段１２に於いて二次暗号化データが「＊％＄＃＝＆％＄＆＃@＋｝｛－＋－／◎×」と一次暗号化データに復号される。

【０１１９】第二復号化手段１２に於いて一次暗号化データに復号後、第一復号化手段１３に於いて、一次暗号化データを第一復号キーを用いて平文に復号化する（Ｓ５６０）。

【０１２０】上記例の場合、一次暗号化データが「＊％＄＃＝＆％＄＆＃@＋｝｛－＋－／◎×」であるので、予め決済システム１又はカード会社から配布された第一復号キーを用いて復号化し、「３５４０１２３４５６７８９」「０１／０５」とカード情報を平文化することとなる。

【０１２１】第一復号化手段１３に於いて復号後、平文化したカード情報をバーチャル加盟店端末１７のカード情報処理手段１６が、正規のカードデータとして復号されているか否かの精査を行い（Ｓ５７０）、精査の結果

何らかの異常が発生している場合には、エラーメッセージをカード情報処理手段１６がユーザ端末１８に送信する（Ｓ５８０）。ユーザ端末１８は、ネットワーク１５を介して受信したエラーメッセージを表示し通知する。

【０１２２】Ｓ５７０の精査の結果異常がなければ、カードリーダー１４が平文化されたカードデータに基づいて電文を編集して、決済システム１に電文を送信する（Ｓ５９０）。ここで電文とは従来のネットワーク１５を介したカード決済と同様に、カード情報を予め定められた形式に変換し、購入商品等のカード決済に対する付随情報と共にカード会社に於いて決済する際の公知のフォーマットに対応したデータをいい、従来のカード決済の際にカード会社に対して送信しているデータと同様のデータを示す。

【０１２３】バーチャル加盟店端末１７からネットワーク１５を介して送信された電文を受信した決済システム１の与信判定手段５は、会員データベース６を参照して当該ユーザに対してカード決済を行っても良いか否かの与信判定を会員データベース６に格納している限度額等の情報に基づいて行い（Ｓ６００）、限度額超過等の理由から決済を認めない場合には、与信拒否報告を与信判定手段５がバーチャル加盟店端末１７のカード情報処理手段１６に送信する。

【０１２４】与信拒否報告を受信したカード情報処理手段１６は、ネットワーク１５を介してユーザ端末１８に与信拒否報告を送信する（Ｓ６１０）。Ｓ６１０に於いて送信された与信拒否報告をユーザ端末１８で受信すると、ユーザ端末１８上に於いて当該ソフトウェアが与信が拒否された旨の与信拒否画面を表示する（Ｓ６２０）。

【０１２５】Ｓ６００の判定の結果、当該ユーザに対して決済を認める場合には、与信許可報告を与信判定手段５がバーチャル加盟店端末１７のカード情報処理手段１６に送信する。与信許可報告を受信したカード情報処理手段１６は、ネットワーク１５を介してユーザ端末１８に与信許可報告を送信する（Ｓ６３０）。Ｓ６３０に於いて送信された与信許可報告をユーザ端末１８で受信すると、ユーザ端末１８上に於いて当該ソフトウェアが与信が許可され、決済が終了した旨の完了画面を表示する（Ｓ６４０）。

【０１２６】このように、Ｓ５００からＳ６４０の一連のプロセスを実行することによって、又バーチャル加盟店端末１７では従来のカード情報処理手段１６に加えて、単に第一復号化手段１３、第二復号化手段１２を併設するのみで、従来よりもセキュリティ性が向上し、且つカード情報処理手段１６からカード会社に於けるカード決済の仕組みには何らの変化も加えずにその処理が可能となる。

【０１２７】本発明に於ける各手段、データベースは、その機能が論理的に区別されているのみであって、物理上あるいは事実上は同一の領域を為していても良い。又データベースの代わりにデータファイルであっても良いことは言うまでもなく、データベースとの記載にはデータファイルをも含んでいる。

【０１２８】尚、本発明を実施するにあたり本実施態様の機能を実現するソフトウェアのプログラムを記録した記憶媒体をシステムに供給し、そのシステムのコンピュータが記憶媒体に格納されたプログラムを読み出し実行することによって実現されることは当然である。

【０１２９】この場合、記憶媒体から読み出されたプログラム自体が前記した実施態様の機能を実現することとなり、そのプログラムを記憶した記憶媒体は本発明を当然のことながら構成することになる。

【０１３０】プログラムを供給する為の記憶媒体としては、例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、磁気テープ、不揮発性のメモリカード等を使用することができる。

【０１３１】又、コンピュータが読み出したプログラムを実行することにより、上述した実施態様の機能が実現されるだけではなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているオペレーティングシステムなどが実際の処理の一部又は全部を行い、その処理によって前記した実施態様の機能が実現される場合も含まれることは言うまでもない。

【０１３２】更に、記憶媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わる不揮発性あるいは揮発性の記憶手段に書き込まれた後、そのプログラムの指示に基づき、機能拡張ボードあるいは機能拡張ユニットに備わる演算処理装置などが実際の処理の一部あるいは全部を行い、その処理により前記した実施態様の機能が実現される場合も含まれることは当然である。

【０１３３】

【発明の効果】本発明によって、このセキュリティ面が向上したことによる、より有効性のあるカード決済を行う決済システム及び方法が可能となった。

【０１３４】更に携帯端末／ユーザ端末を用いた場合、従来はカードリーダーとカード会社とのカード決済用の情報処理システムを変更する必要があったが、本発明を用いることによって、従来のカードリーダーに無線通信とデータ復号化のユニットを単に接続するのみで、カードリーダーとカード会社とのカード決済用の情報処理システムについては何らの変更を加える必要性がない。従って、カード決済用の情報処理システムの変更の手間負担、コスト負担を回避することが可能となる。

【図面の簡単な説明】

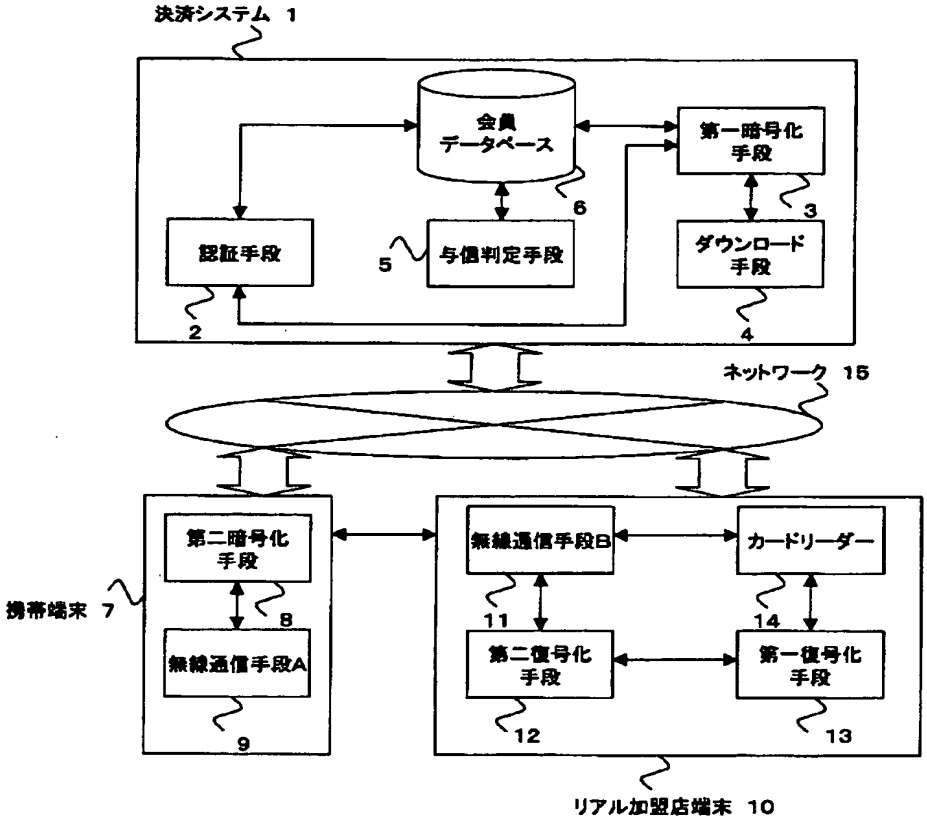
【図１】　本発明のシステム構成の一例を示すシステム構成図である。

【図２】　本発明の他のシステム構成の一例を示すシス

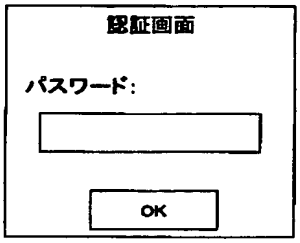
テム構成図である。
【図３】　本発明のプロセスの流れの一例を示すフローチャート図である。
【図４】　本発明のプロセスの流れの一例を示すフローチャート図である。
【図５】　本発明のプロセスの流れの一例を示すフローチャート図である。
【図６】　本発明のプロセスの流れの一例を示すフローチャート図である。
【図７】　本発明のプロセスの流れの一例を示すフローチャート図である。
【図８】　本発明のプロセスの流れの一例を示すフローチャート図である。
【図９】　認証画面の一例を示す図である。
【図１０】購入意思確認画面の一例を示す図である。
【図１１】与信拒否画面の一例を示す図である。
【図１２】完了画面の一例を示す図である。
【符号の説明】

＊１：決済システム
２：認証手段
３：第一暗号化手段
４：ダウンロード手段
５：与信判定手段
６：会員データベース
７：携帯端末
８：第二暗号化手段
９：無線通信手段Ａ
１０：リアル加盟店端末
１１：無線通信手段Ｂ
１２：第二復号化手段
１３：第一復号化手段
１４：カードリーダー
１５：ネットワーク
１６：カード情報処理手段
１７：バーチャル加盟店端末
＊　１８：ユーザ端末

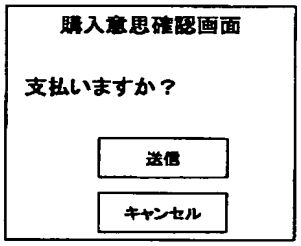
【図１】



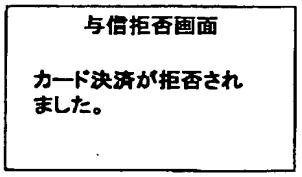
【図９】



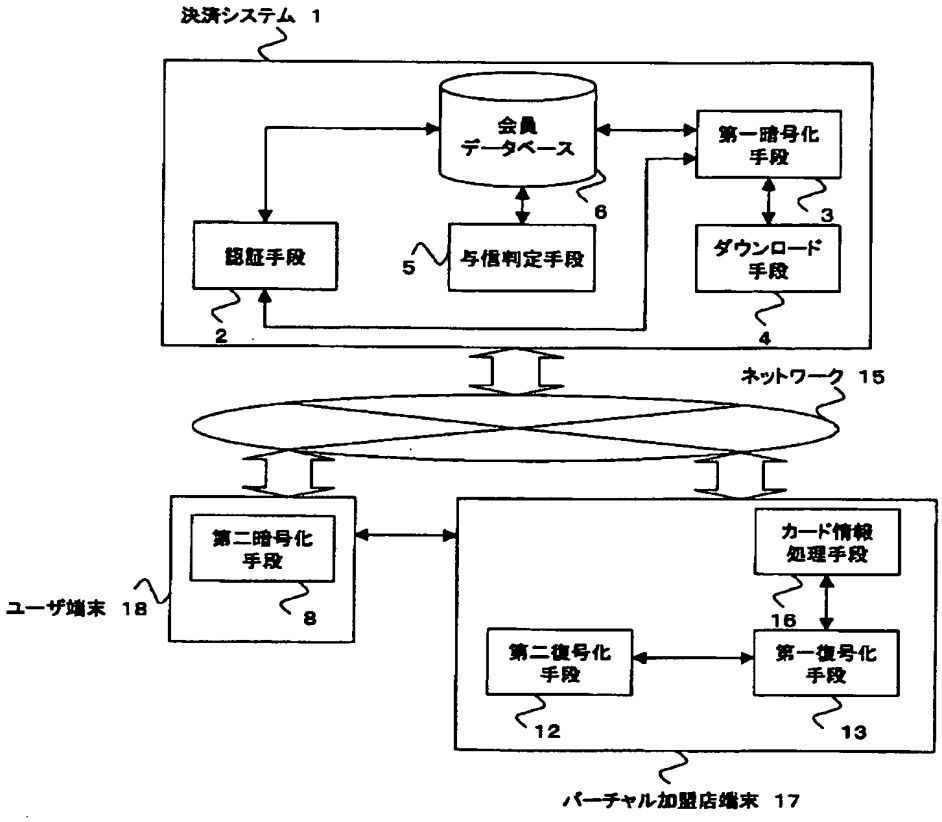
【図１０】



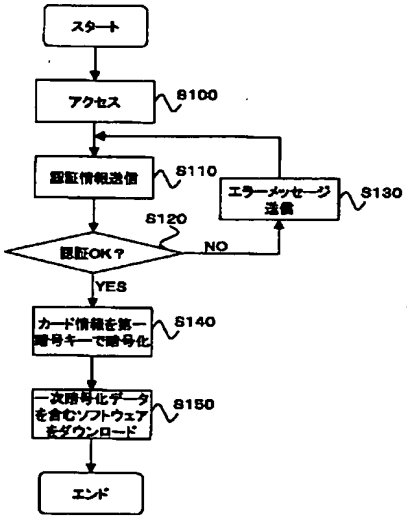
【図１１】



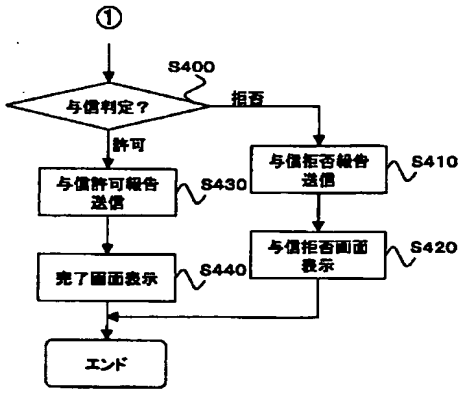
【図２】


決済システム 1
会員データベース
6
第一暗号化手段
3
認証手段
2
与信判定手段
5
ダウンロード手段
4
ネットワーク 15
第二暗号化手段
8
ユーザ端末 18
カード情報処理手段
16
第二復号化手段
12
第一復号化手段
13
バーチャル加盟店端末 17

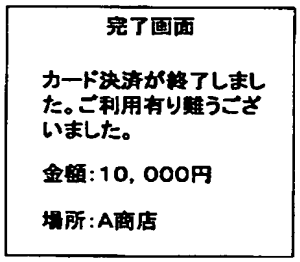
【図３】


スタート
アクセス
S100
認証情報送信
S110
エラーメッセージ送信
S130
S120
認証OK？
NO
YES
カード情報を第一暗号キーで暗号化
S140
一次暗号化データを含むソフトウェアをダウンロード
S150
エンド

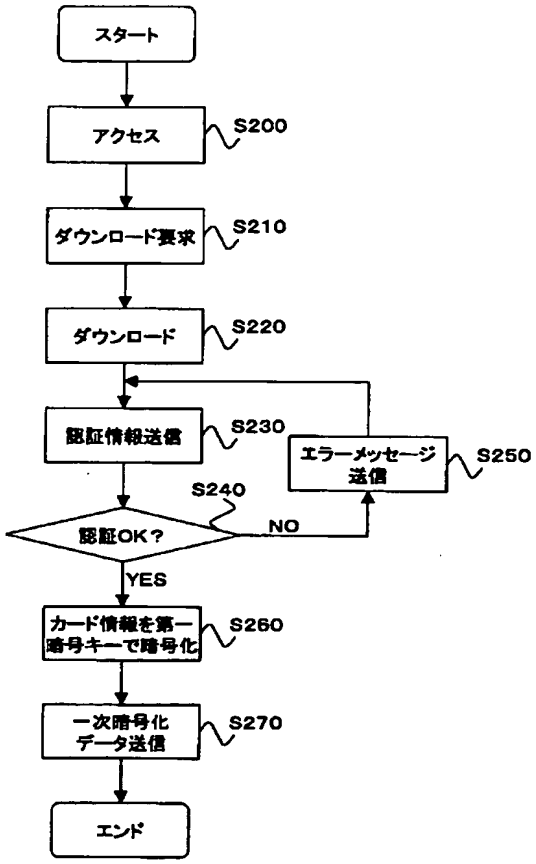
【図６】


①
S400
与信判定？
拒否
許可
与信拒否報告送信
S410
与信許可報告送信
S430
与信拒否画面表示
S420
完了画面表示
S440
エンド

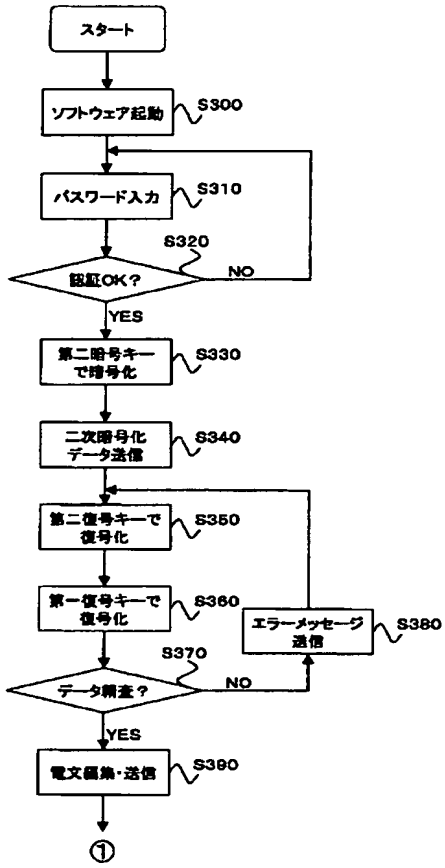
【図１２】


完了画面
カード決済が終了しました。ご利用有り難うございました。
金額：10，000円
場所：A商店

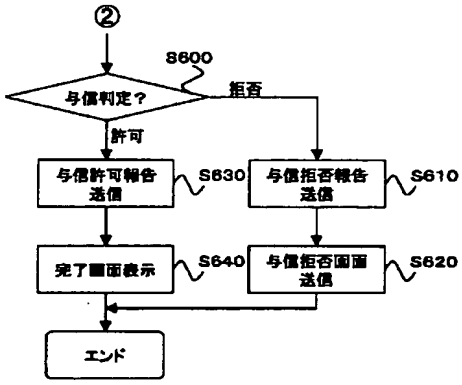
【図４】


スタート
アクセス
S200
ダウンロード要求
S210
ダウンロード
S220
認証情報送信
S230
エラーメッセージ送信
S250
S240
認証OK？
NO
YES
カード情報を第一暗号キーで暗号化
S260
一次暗号化データ送信
S270
エンド

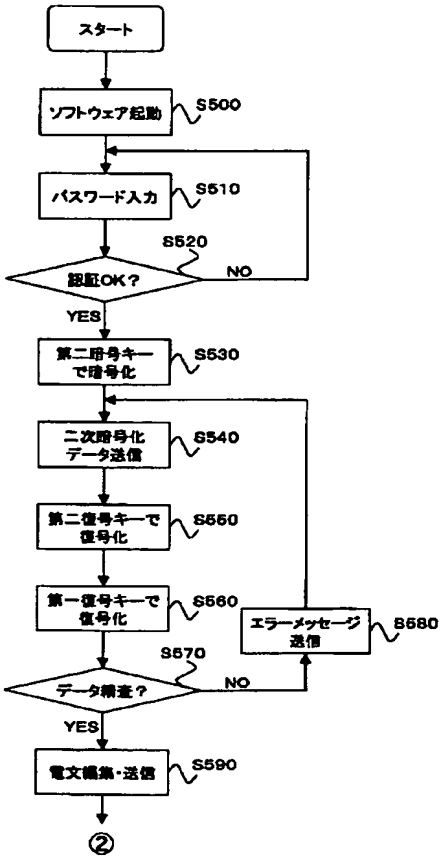
【図５】


スタート
ソフトウェア起動
S300
パスワード入力
S310
S320
認証OK？
NO
YES
第二暗号キーで暗号化
S330
二次暗号化データ送信
S340
第二復号キーで復号化
S350
第一復号キーで復号化
S360
エラーメッセージ送信
S380
S370
データ精査？
NO
YES
電文編集・送信
S390
①

【図８】


②
S600
与信判定？
拒否
許可
与信許可報告送信
S630
与信拒否報告送信
S610
完了画面表示
S640
与信拒否画面送信
S620
エンド

【図７】



フロントページの続き

(51)Int.Cl.'	識別記号	F I	テーマコード (参考)
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ ６６０Ｃ